State of Utah
Technical Architecture
Enterprise Intrusion Detection 2000.08.17

Title: Enterprise Intrusion Detection Standard

Introduction: Intrusion Detection services provide the ability to detect network attacks originating from the Internet. They also provide the ability to quickly shut off network attacks by making changes to the core network routers to deny access from the source device or network where the attack originates. The IDS scanner is a hardware platform that analysis every network packet against knows types of network attacks. Network attacks can be identified by key network characteristics, often called signatures. When a pattern is matched the scanner forwards the information to the IDS director, which provides alarm, notification, and the possibility of modifying router configurations to stop the attack. Common attack signatures are maintained in the scanner and periodically changed or updated. Attached is list of some of the more common signatures the sensor is configured to detect. Additional intrusion detection systems may be installed at State Agencies based upon the requirements identified in Agency Security Needs Analysis documents developed by ITS and related state agencies.

Rationale and Justification: Use of wide area networking (WAN) resources and the Internet has increased the opportunities for foreign access to the network, as well as the opportunity for hackers or unauthorized individuals to connect to State information systems. An enterprise intrusion detection system (IDS) is necessary to monitor, track, and possibly restrict access to the State WAN. Intrusion detection is an essential component of an overall integrated information security plan that also includes firewalls, VPNs, PKI, and Web specific security such as SSL, along with general computer security implementations to guard against unauthorized access and attacks. This standard will assist the State in integrating all these capabilities onto a consistent hardware / software platform to maximize business success and security.

Application: This standard is applicable to all executive government agencies in the State of Utah.

Current Architecture: A few agencies have investigated this technology for application at a Departmental level, however, there has been no enterprise implementations at present. At some locations individual computers have been protected with IDS software such as BlackICE by Network ICE.

Future Architecture: With the explosive growth of the Internet, the need for electronic communications, and the tremendous increase in hacker and security attacks, nearly every agency will recognize the critical need to protect their computing environments from attackers. This will be accomplished in two ways. 1) Implementation of an enterprise IDS system to look for a base level of attacks. 2) Securing individual servers and PCs to make them less prone to attacks. This can be accomplished by more tightly controlled local IDS configurations and/or software and configuration changes on individual computer systems.

Definitions:
Signature: A pattern of network information that can be compared to a rule set indicating typical intrusion activity.

Authority: *Utah Code Section 63D Information Technology Act*.

National and International Standards References: none

Technical Consideration(s): With the installed base of Cisco routers and switches it is imperative that IDS solutions have tight integration with this environment. HP Openview is also utilized extensively at the Enterprise level for network management. The Cisco IDS sensor and IDS Director tightly integrate with these environments allowing for the most flexibility to monitor, notify, and terminate network attacks. The IDS scanner operates on a hardened operating system focused on detecting network intrusion signatures and providing secure alarms to the IDS Director. Future blades for the Cisco Catalyst products will provide integrated IDS capabilities at the switch level. Management of the scanner, future switch blades, and the Director environment is supported at the centralized enterprise level.

Exceptions: Departments are authorized to implement their own network and computer based detection systems to meet the needs of their specific security policies.

Gap Analysis: Specific agency security requirements may identify a need for Departmental IDS capabilities. These requirements can be handled by separate projects and budgeting at the Department level. This does not represent a major impact to the WAN.

Approved Configurations: For the Enterprise installation the Cisco IDS Scanner and IDS Director are deemed necessary. Individual Departmental configurations may utilize this, or other vendor's solutions to meet the specific agency security requirements.

Migration and Implementation Plan: All new purchases of IDS products will be expected to be in full compliance with this standard.

Review Cycle: This standard will be reviewed and updated on an annual basis, based upon the CIO approval date.

State Purchasing Contracts: Cisco IDS products are available under the following contracts:

Contract Number	**Description**	**Vendor**
AR-637	LAN/WAN (US West Router Contract)	Qwest
AR-794	LAN/WAN (US West Switch Contract)	Qwest
AR-877	LAN/WAN Switch Contract	Mountain States Networking

References:

Interim Date: August 17, 2000
Organization Sponsoring the Standard: State Information Security Committee (SISC)
State Technical Architect Approval Date: Pending
CIO Approval Date: Pending
ITPSC Presentation Date: October 19, 2000
Author(s): Joe Leary (ITS)

Addendum: The following is a list of basic attack signatures the IDS Scanner is programmed to detect.

1000 - IP options-Bad Option List
1001 - IP options-Record Packet Route
1002 - IP options-Timestamp
1003 - IP options-Provide s,c,h,tcc
1004 - IP options-Loose Source Route
1005 - IP options-SATNET ID
1006 - IP options-Strict Source Route
1100 - IP Fragment Attack
1101 - Unknown IP Protocol
1102 - Impossible IP Packet
1103 - IP Fragments Overlap
2000 - ICMP Echo Reply
2001 - ICMP Host Unreachable

2002 - ICMP Source Quench
2003 - ICMP Redirect
2004 - ICMP Echo Request
2005 - ICMP Time Exceeded for a Datagram
2006 - ICMP Parameter Problem on Datagram
2007 - ICMP Timestamp Request
2008 - ICMP Timestamp Reply
2009 - ICMP Information Request
2010 - ICMP Information Reply
2011 - ICMP Address Mask Request
2012 - ICMP Address Mask Reply
2100 - ICMP Network Sweep w/Echo
2101 - ICMP Network Sweep w/Timestamp
2102 - ICMP Network Sweep w/Address Mask
2150 - Fragmented ICMP Traffic
2151 - Large ICMP Traffic
2152 - ICMP Flood
2153 - Smurf
2154 - Ping of Death Attack
3000 - TCP Ports
3001 - TCP Port Sweep
3002 - TCP SYN Port Sweep
3003 - TCP Frag SYN Port Sweep
3005 - TCP FIN Port Sweep
3006 - TCP Frag FIN Port Sweep
3010 - TCP High Port Sweep
3011 - TCP FIN High Port Sweep
3012 - TCP Frag FIN High Port Sweep
3015 - TCP Null Port Sweep
3016 - TCP Frag Null Port Sweep
3020 - TCP SYN FIN Port Sweep
3021 - TCP Frag SYN FIN Port Sweep
3030 - TCP SYN Host Sweep
3031 - TCP FRAG SYN Host Sweep
3032 - TCP FIN Host Sweep
3033 - TCP FRAG FIN Host Sweep
3034 - TCP NULL Host Sweep
3035 - TCP FRAG NULL Host Sweep
3036 - TCP SYN FIN Host Sweep
3037 - TCP FRAG SYN FIN Host Sweep
3038 - Orphaned Fin Packet
3039 - Fragmented Orphaned FIN packet
3040 - NULL TCP Packet
3041 - Fragmented NULL TCP Packet
3042 - SYN/FIN Packet
3043 - Fragmented SYN/FIN Packet
3045 - Queso Sweep
3050 - Half-open SYN Attack
3100 - Smail Attack
3101 - Sendmail Invalid Recipient
3102 - Sendmail Invalid Sender
3103 - Sendmail Reconnaissance
3104 - Archaic Sendmail Attacks
3105 - Sendmail Decode Alias
3106 - Mail Spam
3107 - Majordomo Execute Attack

3108 - MIME Overflow Bug
3109 - Q-Mail Length Crash
3150 - FTP Remote Command Execution
3151 - FTP SYST Command Attempt
3152 - FTP CWD ~root
3153 - FTP Improper Address Specified
3154 - FTP Improper Port Specified
3200 - WWW Phf Attack
3201 - WWW General cgi-bin Attack
3201 - WWW General cgi-bin Attack
3201 - WWW General cgi-bin Attack
3201 - WWW General cgi-bin Attack
3201 - WWW General cgi-bin Attack
3201 - WWW General cgi-bin Attack
3202 - WWW .url File Requested
3203 - WWW .lnk File Requested
3204 - WWW .bat File Requested
3205 - HTML File Has .url Link
3206 - HTML File Has .lnk Link
3207 - HTML File Has .bat Link
3208 - WWW campas Attack
3209 - WWW Glimpse Server Attack
3210 - WWW IIS View Source Attack
3211 - WWW IIS Hex View Source Attack
3212 - WWW NPH-TEST-CGI Attack
3213 - WWW TEST-CGI Attack
3214 - IIS DOT DOT VIEW Attack
3215 - IIS DOT DOT EXECUTE Attack
3216 - IIS Dot Dot Crash Attack
3217 - WWW php View File Attack
3218 - WWW SGI Wrap Attack
3219 - WWW PHP Buffer Overflow
3220 - IIS Long URL Crash Bug
3221 - WWW cgi-viewsource Attack
3222 - WWW PHP Log Scripts Read Attack
3223 - WWW IRIX cgi-handler Attack
3224 - HTTP WebGais
3225 - HTTP Gais Websendmail
3226 - WWW Webdist Bug
3227 - WWW Htmlscript Bug
3228 - WWW Performer Bug
3229 - Website Win-C-Sample Buffer Overflow
3230 - Website Uploader
3231 - Novell convert
3232 - WWW finger attempt
3233 - WWW count-cgi Overflow
3250 - TCP Hijack
3251 - TCP Hijacking Simplex Mode
3300 - NetBIOS OOB Data
3301 - NETBIOS Stat
3302 - NETBIOS Session Setup Failure
3303 - Windows Guest Login
3304 - Windows Null Account Name
3305 - Windows Password File Access
3306 - Windows Registry Access
3307 - Windows Redbutton Attack

3400 - Sunkill
3450 - Finger Bomb
3450 - Finger Bomb
3500 - Rlogin -froot Attack
3525 - IMAP Authenticate Buffer Overflow
3526 - Imap Login Buffer Overflow
3550 - POP Buffer Overflow
3575 - INN Buffer Overflow
3576 - INN Control Message Exploit
3600 - IOS Telnet Buffer Overflow
3601 - IOS Command History Exploit
3602 - Cisco IOS Identity
3602 - Cisco IOS Identity
4000 - UDP Packet
4001 - UDP Port Sweep
4002 - UDP Flood
4050 - UDP Bomb
4051 - Snork
4052 - Chargen DoS
4053 - Back Orifice
4054 - RIP Trace
4100 - Tftp Passwd File
4150 - Ascend Denial of Service
4600 - IOS UDP Bomb
5034 - WWW IIS newdsn attack
5035 - HTTP cgi HylaFAX Faxsurvey
5036 - WWW Windows Backup Password File Access Attempt
5036 - WWW Windows Password File Access Attempt
5037 - WWW SGI MachineInfo Attack
5038 - WWW wwwsql file read Bug
5039 - WWW finger attempt
5040 - WWW perl interpreter attack
5040 - WWW perl interpreter attack
5040 - WWW perl interpreter attack
5041 - WWW anyform attack
5042 - WWW CGI Valid Shell Access
5042 - WWW CGI Valid Shell Access
5042 - WWW CGI Valid Shell Access
5042 - WWW CGI Valid Bourne Shell Attack
5042 - WWW CGI Valid Java Shell Attack
5042 - WWW CGI Valid Python Shell Attack
5043 - WWW Cold Fusion Attack
5043 - WWW Cold Fusion Attack
5043 - WWW Cold Fusion Attack
5044 - WWW Webcom.se Guestbook attack
5045 - WWW xterm display attack
5046 - WWW dumpenv.pl recon
5047 - WWW Server Side Include POST attack
5048 - WWW IIS BAT EXE attack
5048 - WWW IIS BAT EXE attack
5049 - WWW IIS showcode.asp access
5050 - WWW IIS .htr Overflow Attack
6001 - Normal SATAN Probe
6002 - Heavy SATAN Probe
6050 - DNS HINFO Request
6051 - DNS Zone Transfer

6052 - DNS Zone Transfer from High Port
6053 - DNS Request for All Records
6055 - DNS Inverse Query Buffer Overflow
6100 - RPC Port Registration
6101 - RPC Port Unregistration
6102 - RPC Dump
6103 - Proxied RPC Request
6104 - RPC Set Spoof
6110 - RPC RSTATD Sweep
6111 - RPC RUSERSD Sweep
6112 - RPC NFS Sweep
6113 - RPC MOUNTD Sweep
6114 - RPC YPPASSWDD Sweep
6115 - RPC SELECTION_SVC Sweep
6116 - RPC REXD Sweep
6117 - RPC STATUS Sweep
6118 - RPC ttdb Sweep
6150 - ypserv Portmap Request
6151 - ypbind Portmap Request
6152 - yppasswdd Portmap Request
6153 - ypupdated Portmap Request
6154 - ypxfrd Portmap Request
6155 - mountd Portmap Request
6175 - rexd Portmap Request
6180 - rexd Attempt
6190 - statd Buffer Overflow
6191 - RPC.tooltalk buffer overflow
6192 - RPC mountd Buffer Overflow
6200 - Ident Buffer Overflow
6201 - Ident Newline
6202 - Ident Improper Request
6250 - FTP Authorization Failure
6251 - Telnet Authorization Failure
6252 - Rlogin Authorization Failure
6253 - POP3 Authorization Failure
6255 - SMB Authorization Failure
6300 - Loki ICMP Tunnelling
6302 - General Loki ICMP Tunneling
8000 - FTP Retrieve Password File
8000 - Telnet-IFS Match
8000 - Telnet-/etc/shadow Match
8000 - Telnet-+ +
8000 - Rlogin-IFS Match
8000 - Rlogin-/etc/shadow Match
8000 - Rlogin-+ +
10000 - IP-Spoof Interface 1
10000 - IP-Spoof Interface 2